By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 2 of 3)

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. There are times that I may also discuss areas of the standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

In my Nov/Dec 2018 article, I discussed CIP-013-1, Supply Chain Risk Management, at a high level. I discussed how I think CIP-013-1 is at the same time plan-based, objective-based, and risk-based. In my Jan/Feb 2019 article I provided a suggested structure for a risk management plan. In this article I'll continue what I began in the Mar/Apr 2019 article, which was a detailed look at the supply chain risk management Requirements for CIP-013-1.

I had planned to cover the supply chain changes to both CIP-005-6, Electronic Security Perimeters, and CIP-010-3, Configuration Change Management and Vulnerability Assessments, in this article, but to allow me to get more in-depth I will cover CIP-010-3 in the Jul/Aug issue as the third part of this now three-part article. Please remember that if you choose to adopt any of my suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

On the May Reliability and Compliance Open Forum Call, I presented a brief overview of the supply chain Standards which includes a slide with links to relevant documents. The presentation from that call is here.

If you want to participate in these monthly calls, the information is on the Compliance Monitoring page of the RF Website.

Malicious Remote Access

Suppose you're the EMS engineer in charge of your primary control system. One afternoon as you're getting ready to go home, you get a call from the operations supervisor. Some of his operators are having trouble with their control consoles. The mouse associated with each console is not working properly. It seems to be moving the display cursor on its own, and not responding to the actual movements of the mouse. As you're speaking, he reports that a breaker controlled by one of the consoles has just been commanded to open. He asks what can be wrong with the systems, and why his operators have suddenly lost control of BES operations. How quickly can you fix this problem and get his operators back in control?

Huron Lightship, Port Huron, MI - Photo by Lew Folkerth

Is this fiction? No. This is the scenario that actually occurred on December 23, 2015, in Kiev, Ukraine (see *Analysis of the Cyber Attack on the Ukrainian Power Grid* here.) And this is the scenario that I believe motivated FERC to address the ability to control vendor remote access. In this article, I'll discuss how the risk of this scenario can be reduced, and how your response can be designed to quickly remediate an actual incursion.

CIP-005-6 R2 Parts 2.4 and 2.5

In Order 829 at P 51-55, FERC required NERC to develop a Reliability Standard to address the risk of vendor remote access to BES Cyber Systems. The new Standard was to cover both interactive and system-to-system remote access. FERC explained that its concerns included malicious use of stolen credentials, possible compromise of a trusted vendor, and use of a vendor's access to compromise or control a BES Cyber System. FERC also stated that an entity

Continued on page 15

Continued from page 14

should be able to "rapidly disable" remote access connections.

CIP-005-6 includes two new Parts. You are required to have methods "for determining" (Part 2.4) and "to disable" (Part 2.5) active vendor remote access sessions. Let's look at the enforceable language of each Part in detail:

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in:

Applicable System	Requirements
High Impact BEC Cyber Systems and their associated PCA; and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA	Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
	Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Let's look at some important points regarding this language:

1. We can look at these Parts as bringing certain Electronic Security Perimeters (ESPs) into scope. All ESPs that contain a high impact BES Cyber System are in scope. All medium impact ESPs that have at least one Electronic Access Point (EAP) associated with the ESP will also be in scope. Within these in-scope ESPs, all Cyber Assets will be in scope. Remember that if any Cyber Asset is within an ESP that has an EAP, the Cyber Asset will almost certainly have External Routable Connectivity (see *The Lighthouse* from Jul/Aug 2015 available here.)

2. Looking at the Requirements, we see we're dealing with several terms not defined in the NERC Glossary. You may need to incorporate your own definitions of any non-glossary terms into your processes and procedures. If you do so, be careful to use commonly accepted definitions and apply them in a way that makes sense in the context in which they're used and that achieves the intent and purpose of the standard.

3. The scope of these Parts includes all data communications into or out of every in-scope ESP, not just routable network traffic. Dial-up, serial leased line, or other communications can also be construed as "remote access," even if it does not employ a routable protocol.

4. These Parts are silent as to how quickly you must be able to respond to an identified issue. In my opinion, identification of malicious remote access sessions and disabling of such access should be achieved in seconds or minutes, not hours or days. If you doubt this, ask your system operators how long a malicious actor should be allowed to control their systems.

5. While the term "vendor" is defined in the Rationale section of the Standard, remember that this section is considered to be guidance and is not enforceable. Rather than be concerned about the precise definition of "vendor," I recommend that, for these Parts, you disregard the term and provide equal consideration for all communications into and out of an in-scope ESP. This will probably be simpler from a compliance perspective and certainly more effective from a security perspective.

6. These Parts are also silent on recovery. I recommend that your processes include methods of capturing forensic evidence, so you can identify the cause of the incursion and correct the weaknesses that led to it. As any malicious remote access meets the definition of a Cyber Security Incident, your CIP-008 incident response plan should be activated. Make sure the incident response plan has provisions for dealing with cases of malicious or unauthorized remote access. Also, when recovering systems back to normal operating mode your CIP-009 recovery plan may need to be invoked. Ensure it has provisions for these circumstances.

Continued on page 16

Continued from page 15

How can you control remote access in a manner that meets the security objective of Parts 2.4 and 2.5? I suggest a layered approach to this problem:

Identification:

Control of remote access traffic begins with understanding all traffic that crosses the ESP border, including any traffic that bypasses the ESP border such as dial-up or serial communications. You should already have a good handle on this from the existing CIP-005-5 Requirements, but I think it's time to revisit this topic in more depth. You should clearly understand (and document) the need for each type of traffic permitted into or out of the ESP.

What are the endpoints of the traffic, the source and destination, and what service is provided?

Who uses this service, and why is it needed?

Which firewall rules permit this traffic?

How does it contribute to reliability? What would be the impact if the traffic is blocked?

If the far endpoint for this traffic is compromised, can this traffic be used to compromise BES reliability?

All of these questions should be answered and documented for use in the items below.

Categorization:

Once you identify the traffic, you should categorize the traffic based on reliability need. Consider these as possible categories for your traffic:

- Required for operations under all conditions, normal and emergency
  - This traffic will probably include ICCP feeds to your BA, RC, and/or TOP. It will also probably include monitoring and control links between Control Centers and field devices like a substation RTU or a generator DCS.

- Required for normal operations, but may be suspended for emergencies
  - This category might include engineering workstation access into the production network for routine maintenance and configuration. Traffic that is part of a historian system that is not used for situational awareness might also be included here.

- Convenience connections, not necessary but useful for saving time or labor
  - Most Interactive Remote Access probably falls here, such as engineering connections from home to permit after-hours response.

- Other connections
  - In my opinion, there should be no traffic in this category. If it doesn't support operations, and doesn't save time or labor, why is it permitted into or out of the ESP?

Classification:

Classify the traffic by the type of party you're communicating with:

- Internal: Communication is within your entity's networks or within secure communication links between such facilities.

- Registered Entity: Communication is to another Registered Entity (BA, TOP, etc.).

- External Party: Communication is to another party not subject to the CIP Standards. I consider this traffic to be "vendor" traffic.

Prioritization:

Determine which traffic must be kept operational under various conditions. You might develop three conditions of operation: normal conditions (no suspected threat), heightened security (response to a suspected threat), and maximum security (response to a probable or confirmed active threat).

Response Preparation:

There are some actions you can take to proactively reduce your exposure to remote access threats.

- Architecture:

  Your vendors should not have direct access into your ESPs. If a vendor must have remote access, consider giving your vendor access to a test or QA environment rather than the production control systems. To the greatest extent possible, modify your architecture so that only traffic that is absolutely necessary is permitted into the ESP.

Continued on page 17

Continued from page 16

- Network Configuration:

  You should review your network configuration to determine if modifications can increase the isolation of systems that are capable of remote access. For example, it may be possible to restrict the network visibility of a console that is the target of Interactive Remote Access by placing it on its own VLAN internal to the ESP and restricting traffic to and from that VLAN to the rest of the ESP. This type of segmentation can be valuable in increasing security, but be careful that it doesn't disrupt operations.

- Simplification:

  There may also be opportunities to prevent traffic from crossing the ESP boundary. Services such as Active Directory or network printing could be moved to dedicated devices within the ESP to prevent that traffic crossing the ESP boundary. Analyze this type of change carefully to make sure you are actually improving overall security.

- Security Appliances:

  You may be able to incorporate security systems such as a Security Information and Event Management system or Intrusion Detection System into your remote access protections. Remember, though, that you are after very fast response times and there may not be time to run reports or do extensive analysis.

Response Planning:

Once you know your traffic and have optimally configured your networks, you should plan your response scenarios. At a minimum, you must be able to turn off access to any traffic classified as "vendor" traffic above. A good way to organize the response is to incorporate the prioritization levels identified above. Your target here is to get maximum improvement in security for a minimum in response time. To me, this indicates the need for pre-planned and pre-tested configuration changes that can be implemented with minimum risk to reliability.

These configuration changes should be manually-initiated automated processes so that manual processes don't slow the response or introduce errors in the network configuration. In planning for this type of response, be sure to consider your change control processes.

You don't want to have a required change approval slow down your response to an emergency. Test your automated processes thoroughly. The goal is to improve reliability, but these processes could also have unintended consequences if not properly vetted.

Training and Exercises:

Ensure all personnel who will be responsible for recognizing and reporting instances of malicious or unauthorized remote access are trained in these skills and that their training stays fresh. Ensure the personnel who are to receive these reports are confident and proficient in their roles so they can respond quickly and properly to any identified incursion. Frequent exercises will help with this.

How you detect a remote intrusion and how you disable any such detected access will depend greatly on your position in the BES, on the systems you use, and on your personnel. While I don't have specific advice for detecting and disabling malicious connections that defeat your protective measures, I do believe the planning and preventive actions I've described above will help.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

I may be reached here.